Testimony of Dr. Igor Khripunov
Associate Director
Center for International Trade and Security
University of Georgia in Athens
Before the
U.S. House Committee on Homeland Security
Subcommittee on Prevention of Nuclear and Biological Attack

"New Opportunities for Reducing Nuclear and Biological Threats at the Source"

June 22, 2006

Thank you, Mr. Chairman and other distinguished members of the Subcommittee. I am pleased to have this opportunity to describe my work in the area of the "human factor," which is becoming increasingly important as we attempt to implement effective threat-reduction programs. Simply put, the human factor emphasizes that the skill and élan of security personnel are the critical element in security. Equipment is not enough.

In the new strategic environment of the 21st century, "asymmetric warfare" has become a common buzzword. For those entrusted with protecting critical infrastructure and materials at the source, asymmetric threats imply attempts by adversaries to circumvent or undermine our strengths while exploiting our weaknesses using methods that differ significantly from traditional methods of operation. Asymmetric attacks employ innovative, nontraditional tactics, weapons, and technologies; thus they demand a spectrum of protective strategies on our part.

But no strategy, however well-conceived, can prepare the staffs of sensitive sites for every contingency. More than ever before, the protective force will depend on such professional skills and traits as situational awareness, strength of mind, mental readiness, boldness, self-reliance, intuition, and a willingness to take risks. In the kind of confrontations we envision, these characteristics are imperative. They will help security forces at sites housing lethal materials expect the unexpected and react adequately under conditions of extreme stress and uncertainty.

Security Culture

The concept of the human factor originated with a simple insight: that the best equipment in the world is no better than its operator. Nor can the best written directives in the world compensate for apathy or technical incompetence in the workforce. These material arrangements have little effect without trained, motivated human beings to make use of them. A vehicle to improve the human factor is "security culture," a concept that encompasses a set of managerial, organizational, and other arrangements. When we set out to improve security culture within an organization active in the nuclear or biotechnology complex, we set out to cultivate habits, attitudes, and traditions that favor security over lesser concerns. Security becomes second nature for personnel within such organizations.

This type of organizational culture is tightly based on the concept of nuclear security which is defined by the International Atomic Energy Agency (IAEA) as the prevention and detection of,

and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. This definition has important and extensive overlaps with chemical and bio security.

On our side of the asymmetrical-warfare equation, where dangerous gaps and vulnerabilities have become apparent, we can come up with a state-of-the-art multidisciplinary methodology to prepare the workforce for both actual and potential threats. Hence, security culture connotes not only the technical proficiency of the people assigned security-related duties, but also their willingness and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise—as they will, given the limits on human foresight and the inventiveness of the adversaries we face today.

In this sense, then, a good security culture can be defined as a work environment where an ethic of security permeates the organization. People's behavior focuses on preventing malicious acts through critical self-assessment, aggressive efforts to identify management and tactical problems, and appropriate, timely, and effective resolution of problems before they become crises. Security culture enables a person to respond to known and unknown security risks out of carefully nurtured and proactive habit rather than improvised effort.

There are two categories of unexpected events of which we need to be aware and for which security culture may be an effective tool. First, a known danger whose timing or magnitude cannot be predicted has been dubbed a "known unknown." Second, there are other dangers called "unknown unknowns." Nobody is aware of these. Nobody will foresee them or take countermeasures until they transpire. Crashing fuel-filled passenger jets into the World Trade Center towers on September 11, 2001 represented a striking example of an unknown unknown.

Every organization has a security culture. (Incidentally, the same could be said of safety, quality, and other fields of endeavor.) The really important question is: Is the security culture healthy? Is it what management needs it to be, and is it improving, decaying, or remaining static? How effectively does it counteract security breaches and insider threats? How can it be improved?

As we survey the world, we find numerous examples showing that a group of unscrupulous employees—typically managers colluding with lower-ranking technicians—can divert and steal valuable, sensitive, and dangerous materials from the workplace despite seemingly airtight security and anti-theft precautions. One representative case involved a criminal operation at Elektrokhimpribor, a top-secret nuclear-weapons facility in Russia's closed city of Lesnoy. Thefts of rare and expensive radioactive isotopes went on unchecked for several years because employees from all levels at the facility—ranging from rank-and-file workers to top management—connived among themselves, abetted by senior officials from the Ministry of Atomic Energy (the federal agency charged with overseeing security at such sites).

Under a different set of circumstances in Pakistan, had there been a chance to promote security culture values throughout its national nuclear sector, some members of the workforce might have found A.Q. Khan's shady nuclear transactions with proliferant entities objectionable and inconsistent with world standards, prompting them to blow a whistle. Ambassador Linton Brooks, administrator of the National Nuclear Security Administration, delivered a presentation

at the Congressional Breakfast Club on May 19, 2006 in which he acknowledged that "every security system ultimately depends on the people operating it—the so-called 'human factor.' Motivated by greed, coercion, or debt, facility insiders may successfully divert nuclear materials."

Nor is the United States immune to faults in security culture that can render nuclear facilities vulnerable to terrorist and other malicious acts. On August 29, 2004, CBS News reported that officials from the U.S. Department of Energy had conducted an surprise inspection of security guards at a nuclear-weapons plant in Colorado, finding the facility virtually unprotected because the vast majority of the guards were watching the Super Bowl. The Department of Energy admitted that guard forces had recently left the front gates at other nuclear facilities wide open, and that they had failed repeatedly to respond to emergency alarms in maximum-security areas. Some were actually caught sleeping on the job.

Sectoral Diversity

A concept of security culture originated within the IAEA and the nuclear sector. Twelve "fundamental principles" of nuclear security were developed immediately after the 9/11 attacks and are now codified in a series of (as-yet unratified) amendments to the 1980 Convention on the Physical Protection of Nuclear Material. The basic concept and methodology of security culture continues to undergo refinement by the IAEA Secretariat, but it can be usefully applied to other sensitive areas, such as the biological and chemical sectors, in which breaches of security may hand deadly materials to terrorists, posing a threat to the public.

- *Nuclear*. Emerging security challenges have made it obvious that the scope of nuclear security and the associated culture need to extend beyond the traditional task of protecting weapons-usable material. This new, more comprehensive security culture must cover radioactive sources and spent nuclear fuel, among other hazardous radiological substances, while encompassing a wide variety of installations and activities. It must account not only for power and research reactors and related fuel-cycle facilities, but also for waste storage sites that serve research, academic, agricultural, and industrial installations.

  Of special significance is nuclear power infrastructure. An attack on a nuclear power site would likely lead to serious consequences, even if little or no damage were done to the plant itself or to related structures. Public fears of radiation, combined with a possible massive blackout and other aggravating factors, could give rise to significant distress and panic. In other words, even a marginally successful terrorist attack on nuclear plant infrastructure could easily bring about a systemic disaster, characterized by a series of interconnected and disruptive events affecting vital societal institutions.

  In July 2005, the parties to the Convention on the Physical Protection of Nuclear Material approved a series of amendments to the Convention. Among other things, the amendments raise the 12 fundamental principles of nuclear security to the level of binding obligations under international law. Although security culture is listed alongside principles such as threat evaluation, a graded approach, defense-in-depth, and quality

assurance—implying coequal status—it is clear that culture stands above them all. It is an overarching and integrating concept without which none of the other fundamental principles can be successfully implemented.

The amendments make the fundamental principles of nuclear security universal and binding, and they give the international community a way to hold individual governments accountable for their performance in this critical area. In this light, it is disturbing that only three countries (the Seychelles, Turkmenistan, and Bulgaria) have ratified the amendments almost a year after they were signed. It is clearly in the interest of the United States to invest time and resources in efforts to accelerate the ratification process, both in Congress and abroad, helping the amendments to the Convention enter into force at an early date.

- *Chemical*. Among the threats to the chemical industry and to chemical-weapons storage/destruction facilities are deliberate attempts to release toxic materials while they are in transit to or from points of storage or use; theft or diversion of chemical weapons or toxic materials for terrorist acts elsewhere; and sabotage that releases toxic contaminants, in effect using chemical installations as weapons prepositioned in urban areas. A multitude of industrial chemicals, though not as deadly as chemical-warfare agents, could be released in massive quantities, inflicting lethal effects despite their lower toxicity.

  A classified study conducted by the U.S. Army Surgeon General, dated October 29, 2001, projected that a terrorist attack dispersing toxic chemicals in a densely populated area could injure or kill as many as 2.4 million people. (The Army later clarified its findings, noting that the estimate of 2.4 million casualties referred to the number of people who might request medical treatment following a large-scale release from a chemical manufacturing plant, in a densely populated area, under ideal weather conditions that lent themselves to maximum exposure.) If nothing else, however, this attests to the psychological impact of chemical incidents, which would exacerbate the actual, measurable damage to infrastructure and human health.

  What kind of substances might be released? Chlorine and phosgene are two industrial chemicals commonly transported by road and rail. They are also chemical-warfare agents, having seen widespread use in World War I. Rupturing the containers in which they are transported could disseminate these gases in incapacitating or lethal amounts. Organophosphate pesticides such as parathion fall into the same class as nerve agents. Although these pesticides are far less toxic than military-grade nerve agents, their effects and medical treatments are the same. In April 2005, Dr. Richard Falkenrath, President Bush’s deputy homeland security advisor, told the Senate Committee on Homeland Security and Governmental Affairs that, of all the capabilities available to terrorists in the United States today, one stands alone as uniquely deadly, pervasive, and susceptible to terrorist use: industrial chemicals such as chlorine, ammonia, phosgene, methyl bromide, hydrochloric acid, and various other acids.

In contrast to the nuclear sector, which is made up of relatively few facilities equipped with costly and sophisticated protective systems, sensitive chemical plants number in the thousands and, generally speaking, are only lightly protected. To an even greater degree than in the nuclear industry, accordingly, physical protection in the chemical industry depends not so much on the design and condition of installed security equipment as on the attitudes, behavior, and motivation of the entire workforce. In the long run, human performance, influenced by prevailing standards of security culture, determines whether a chemical security regime succeeds or fails. The sheer scale of the chemical industry increasingly makes security culture, including the vigilance of the workforce, a key element in protecting hazardous facilities and chemicals.

A recently released report from UN Secretary General Kofi Annan, titled *Uniting Against Terrorism: Recommendations for a Global Counter-Terrorism Strategy* (A/60/825, April 27, 2006) appropriately emphasizes that:

> To prevent terrorists from acquiring chemical materials, States should ensure that security at chemical plants is kept to the highest standard, and I urge the relevant United Nations entities to provide assistance where needed. A mechanism should also be developed to allow the Organization for the Prohibition of Chemical Weapons (OPCW), in cooperation with other relevant United Nations actors, to provide necessary assistance and coordinate the response and relief operations in case of a chemical weapon attack or the release of chemical agents.

Indeed, the OPCW, a worldwide authority on chemical weapons, is best equipped to become a clearinghouse and coordinating center for chemical security culture. Its expertise, knowledge, and equipment can be put to use preventing, combating, and responding to chemical terrorism. The Chemical Weapons Convention, the document under which the OPCW operates, clearly provides the organization with a mandate not only to deal with chemical weapons narrowly construed, but also to foster security in the chemical sectors of member states.

- *Biological*. At biotechnology labs and pharmaceutical plants, the role of the human factor is even greater than in the nuclear and chemical complexes because of the ease with which an unscrupulous staff member could divert pathogen samples from their proper uses. Preventing bioterrorism requires innovative solutions specific to the nature of the threat. Biotechnology is not like nuclear technology. Soon, tens of thousands of laboratories worldwide will be operating in this multi-billion-dollar industry. Even students working in small laboratories will be able to carry out gene manipulation. A minute amount of pathogens can be used to create a sizable stock of weapons-usable material. The approach to fighting the abuse of biotechnology for terrorist purposes will have more in common with measures against cyber-crime than with our work to control nuclear proliferation. As a result, biosecurity culture is substantively and structurally different from security culture in the nuclear and chemical complexes.

  There is a compelling need to forge a voluntary code of conduct for the biotech industry, governed by the principles of risk management, ethical values, and strict compliance.

Personnel accountability is a major trait to be nurtured at these institutions. Members of the workforce must always bear in mind the potential consequences of the firm's research, recognizing the repercussions that would accrue were their scientific endeavors misused. Because biosecurity depends so heavily on vigilance and on expecting the unexpected, top leaders must encourage their workforces to be observant and to question small discrepancies as a matter of routine. Effective biosecurity would include an oversight system for (a) the physical protection of dangerous pathogens and dual-use technologies from theft, illicit sale or transfer, or accidental release; (b) the implementation of security regulations; (c) safety training; (d) facility licensing; and (e) personnel vetting.

Here again, the human factor is the key to success in biosecurity culture, even though it may require more effort and time to nurture. Since the dividing line between biological weapons and naturally occurring infectious diseases is blurry, the United States may wish to turn to the World Health Organization (WHO), encouraging that body to strengthen and diversify its involvement in this area. This would make the WHO the biosecurity counterpart to the IAEA and the OPCW. It would also enhance preparations for natural outbreaks such as bird flu. It will be necessary to focus on raising standards of biosecurity culture, both to protect the general public from naturally occurring disease and to shield our citizens against malicious acts.

Building Security Culture

Cultures are based on a set of shared, underlying assumptions about reality. Practically speaking, this means that an organization instills tangible behaviors in the workforce that derive from what the organization's leaders assume should be most important. Even if the leadership makes the right assumptions and sets the right goals, however, culture will atrophy unless the leadership works actively and continuously to promote them throughout the organization. Without proactive leadership, the staff will simply form other assumptions based on individual staff members' personal experiences, or even on their whims. Top managers need to lead the way in forging the appropriate pattern of ideas. Often underlying assumptions are unconsciously held and never discussed in the daily course of business. They simply become "the way we do things." But a culture needs conscious attention if it is to thrive.

A good security culture is founded on a healthy respect for the threat. From the most senior leader down to the lowliest technician, the staff needs to understand that security measures truly matter. This underlying conviction then permeates the way people work, and it drives their behavior under normal and abnormal conditions. In a facility that enjoys a healthy security culture, personnel typically display a deep-rooted belief that there are credible insider and outsider threats, including theft, sabotage, unauthorized access, illegal transfer, and other malicious acts, and that it is their duty to counteract those threats. A sense of mission goes a long way toward fissile-material security, as well as the security of pathogens and toxic chemicals.

The next level in implanting healthy assumptions is to determine basic principles and values conducive to the behaviors and physical arrangements that make up a vibrant security culture. The necessary principles and values include honesty, integrity, and a sense of responsibility; a

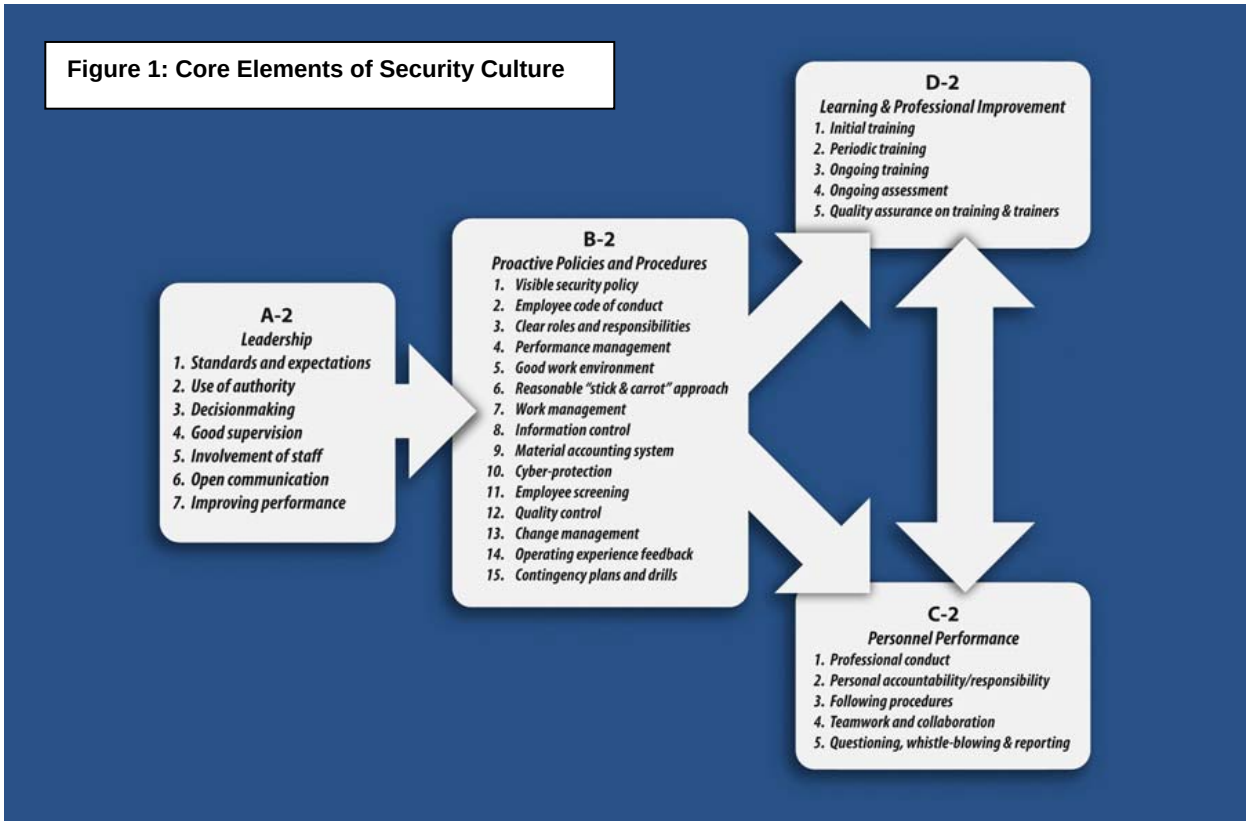
commitment to keeping equipment in good working order; obedience to procedure; a commitment to learning and process improvement; and effective leadership throughout the organizational hierarchy. These traits contribute to the core of security culture.

The core consists of four major elements: (1) facility leadership, (2) proactive policies and procedures, (3) personnel performance, and (4) learning and professional improvement. (See Figure 1, next page.) But the main element within the facility is the performance of leaders. Top managers are responsible for developing and implementing a specific set of policies and procedures that bias the behavior of their subordinates in favor of security. Of particular importance to the core is a manager's emphasis on clear roles and responsibilities, visible security policies, cyber-protection, contingency plans and drills, and personal accountability. Continuous training is the primary tool to get the required results.

These desired traits are not, of course, confined to security; they are mainstays of healthy management practices. Conversely, a poorly managed work environment in which these attributes are lacking will be indifferent to efforts to achieve a high standard of security culture. Accordingly, any campaign to promote nuclear security culture—whether nationally sponsored or funded primarily through international assistance—should seek to better the overall professional culture.

It is in U.S. national interest to take the lead in supporting and promoting security culture not only domestically but also internationally, making its basic standards universally understood, regardless of differing socioeconomic and political conditions from country to country. A uniform understanding of clearly defined standards is important for international exchanges, evaluation, and comparison. A good example of such highly beneficial outreach is the U.S.-Russian program on security culture currently implemented under the bilateral Statement on Nuclear Security Cooperation signed by Presidents George W. Bush and Vladimir Putin at their summit meeting in Bratislava, Slovak Republic, in February 2005. Ideally, this must serve as a powerful tool for shaping the mindset of nuclear workforce in Russia and pave the way for similar efforts in other countries.

Indeed, there is an urgent need to engage, either bilaterally or through the IAEA, a specific group of countries whose history, traditions, ongoing economic developments, and other traits complicate their ability to meet high standards of security culture. This group includes transitional societies, countries whose nuclear programs lacked or still lack transparency, countries instituting nuclear power and research programs from scratch, or where nuclear industry is undergoing ownership reform. For example, countries professing a desire to benefit from nuclear power generation, such as Turkey, Vietnam, Indonesia and Nigeria, need to start training a security-conscious workforce even before they design and build appropriate physical infrastructure.



Beyond the Source

Security culture is no panacea. It cannot credibly prevent the whole spectrum of terrorist attacks involving weapons of mass destruction (WMD). Though we stand a reasonably good chance of denying terrorists access to nuclear weapons and to the material and technologies they would need to build an improvised nuclear device (IND), most components for radiological terrorism or bioterrorist attacks are easily available and technologically simple to use. They stand out among the WMD tools available to terrorists both because of their ready availability and because of their unique capacity to inflict far-reaching physiological and psychological damage.

Compared to nuclear weapons and INDs, radiological weapons require little technical sophistication. The probability that such weapons will be used is on the rise: Conventional terrorism seems to be gradually losing its attractiveness to perpetrators as public authorities take defensive precautions and ordinary citizens demonstrate more resilience in the face of its disruptive effects. From a symbolic standpoint, moreover, al Qaeda and its ilk would be tempted to use radiological weapons because they resemble nuclear weapons, thus conferring prestige and an image of prowess on their efforts and heightening anxieties among the populace targeted for attack. Similarly, acts of bioterrorism can be prevented and mitigated only in a limited way, but they could have long-lasting and indiscriminate effects, raising the specter of a global pandemic.

Any new efforts to prevent the proliferation of weapons-usable materials at the source must be combined with efforts to prepare ordinary citizens for acts of WMD terrorism that are less

preventable. This balanced formula must include a strategy to build up a culture of resilience among the public, which after all is a primary target for terrorists. Resilience refers to the ability to handle disruptive challenges, characterized as emergencies that can result in crisis. Accordingly, resilience culture is an amalgam of beliefs, attitudes, approaches, behaviors, and psychology that helps people fare better during adversity. Resilient people bend rather than break under stressful conditions, and they return to some semblance of their normal psychological and social routine following misfortune.

The challenge of terrorism demands a global response, as compassionate to victims as it is resolute in seeking out and defeating perpetrators. Security culture at the source, complemented by public resilience, offers a foundation for a partnership and strategy that will help deny terrorists their goals. Our efforts in this area will help us fortify ourselves for the long war that confronts us.